(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－124952
（P2002－124952A）
(43)公開日　平成14年４月26日(2002.4.26)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　12/28		Ｈ０４Ｌ　11/00	３１０Ｂ	５Ｊ１０４
Ｈ０４Ｑ　7/38		Ｈ０４Ｂ　7/26	１０９Ｒ	５Ｋ０３０
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ｃ	５Ｋ０３３
9/32			６７５Ａ	５Ｋ０６７
12/56			６７５Ｄ	

審査請求　未請求　請求項の数２　ＯＬ　（全　６　頁）　最終頁に続く

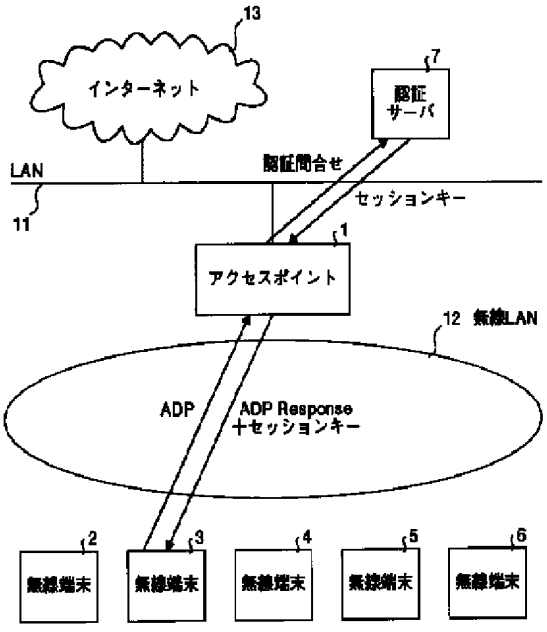
(21)出願番号　特願2000－312626(P2000－312626)
(22)出願日　平成12年10月12日(2000.10.12)

(71)出願人　000005290
古河電気工業株式会社
東京都千代田区丸の内２丁目６番１号
(72)発明者　福富　昌司
東京都千代田区丸の内２丁目６番１号　古河電気工業株式会社内
(72)発明者　太田　昌孝
東京都目黒区大岡山２－12－１
(74)代理人　100089118
弁理士　酒井　宏明

最終頁に続く

(54)【発明の名称】　無線ネットワークにおける無線端末の認証方法および無線ネットワークにおける無線端末の認証システム

(57)【要約】
【課題】　パケットフォーマットを変更することなく、不正なユーザによる不正アクセスを防止して、ネットワークリソースの不正利用を回避すること。
【解決手段】　無線端末２～６は、最初にリクエストを送信する。基地局１は、リクエストを中継し、送信元のＭＡＣアドレスを取り出して、端末の認証を行うためのパケットを認証サーバ７に送信し、認証サーバ７は、ＭＡＣアドレスを受信すると、暗号化を行ったセッションキーを送信する。続いて、基地局１は、セッションキーを保存し、レスポンスのパケットにセッションキーをつけて送信し、無線端末２～６は、セッションキーを保存し、以降、ＣＲＣ値の計算をＭＡＣのヘッダ、ペイロードにセッションキーを加えたハッシュ値を元に計算してパケット送信する。基地局１は、受信時にセッションキーを使って、ＨＡＳＨ値を加えたＣＲＣ計算の値とパケットのＣＲＣの値を比較してパケット単位の認証を実現する。



【特許請求の範囲】
【請求項１】　複数のＬＡＮと、各ＬＡＮに対応する複数のルータまたはブリッジと、バックボーン網により構成され、各ＬＡＮは対応するルータまたはブリッジにより前記バックボーン網を介して互いに接続され、各ＬＡＮは基地局と１つ以上の無線端末を含む無線ネットワークにおける無線端末の認証方法であって、
前記無線端末は、最初に通信を開始するにあたり、ＡＲＰのリクエストまたはＤＨＣＰのリクエストを送信し、
前記基地局は、そのリクエストを中継すると共に、送信元のＭＡＣアドレスを取り出して、認証サーバに対して端末の認証を行うためのパケットを送信し、
前記認証サーバは、ＭＡＣアドレスを受信すると、あらかじめ配布しているシークレットキーで暗号化を行ったセッションキーを送信し、
前記基地局は、セッションキーを保存すると共に、ＡＲＰのリプライまたはＤＨＣＰのレスポンスのパケットに、セッションキーをつけて送信し、
前記無線端末は、受信したセッションキーを保存し、以降のパケット送信では、ＣＲＣ値の計算をＭＡＣのヘッダ、ペイロードにセッションキーを加えたハッシュ値を元に、計算してパケットを送信し、
前記基地局は、パケット受信時に、保存しているセッションキーを使って、同様のＨＡＳＨ値を加えたＣＲＣ計算の値とパケットのＣＲＣの値を比較することで、パケット単位の認証を実現することを特徴とする無線ネットワークにおける無線端末の認証方法。
【請求項２】　複数のＬＡＮと、無線端末の認証を行う認証サーバと、バックボーン網とにより構成され、各ＬＡＮおよび認証サーバは対応するルータまたはブリッジにより前記バックボーン網を介して互いに接続され、各ＬＡＮは基地局と１つ以上の無線端末を含む無線ネットワークにおける無線端末の認証システムであって、
前記無線端末は、最初に通信を開始する場合に、ＡＲＰのリクエストまたはＤＨＣＰのリクエストを送信する第１の送信手段と、前記基地局から受信したセッションキーを保存する第１の保存手段と、ＣＲＣ値の計算をＭＡＣのヘッダ、ペイロードにセッションキーを加えたハッシュ値を元に、計算してパケットを送信する第２の送信手段と、を備え、
前記基地局は、前記無線端末からのリクエストを中継すると共に、送信元のＭＡＣアドレスを取り出して、前記認証サーバに対して端末の認証を行うためのパケットを送信する第３の送信手段と、前記認証サーバから受信したセッションキーを保存する第２の保存手段と、ＡＲＰのリプライまたはＤＨＣＰのレスポンスのパケットに、セッションキーをつけて送信する第４の送信手段と、パケット受信時に、前記第２の保存手段で保存しているセッションキーを使って、同様のＨＡＳＨ値を加えたＣＲＣ計算の値とパケットのＣＲＣの値を比較してパケット単位の認証を行う認証手段と、を備え、
前記認証サーバは、ＭＡＣアドレスを受信すると、あらかじめ配布しているシークレットキーで暗号化を行ったセッションキーを送信する第５の送信手段を備えたことを特徴とする無線ネットワークにおける無線端末の認証システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、複数のＬＡＮと、各ＬＡＮに対応する複数のルータまたはブリッジと、バックボーン網により構成され、各ＬＡＮは対応するルータまたはブリッジによりバックボーン網を介して互いに接続され、各ＬＡＮは基地局と１つ以上の無線端末を含む無線ネットワークにおける無線端末の認証方法および無線端末の認証システムに関する。
【０００２】
【従来の技術】無線ＬＡＮの方式は、ＩＥＥＥ８０２．１１として標準化がなされており、アクセス方式はＣＳＭＡ／ＣＡ（Carrier Sense Multiple Access with CollisionAvoidance）である。基本的に端末局は自由に通信を行うことが可能であり、特に通信を開始するための認証手順はない。また、直接シーケンススペクトラム拡散方式では、利用する拡散コードを管理することで通信できる相手を特定することは可能であるが、一般に同一種類の製品では同一の拡散コードを使い、上位層の認証に利用できるような使い方はされない。
【０００３】
【発明が解決しようとする課題】このような無線ＬＡＮのシステムをアクセス網として利用する場合、契約者でない不正なユーザでも、容易にネットワークに接続することが可能であるため、ネットワークリソースの不正利用が可能であるという問題点があった。
【０００４】また、不正アクセスを回避するために、パケットフォーマットに変更を行うと、データリンクの最大転送可能データ長に影響がでるため、パケットフォーマットの変更を容易に行えないという不都合もあった。
【０００５】本発明は上記に鑑みてなされたものであって、パケットフォーマットを変更することなく、不正なユーザによる不正アクセスを防止して、ネットワークリソースの不正利用を回避することを目的とする。
【０００６】
【課題を解決するための手段】上記の目的を達成するために、請求項１に係る無線ネットワークにおける無線端末の認証方法は、複数のＬＡＮと、各ＬＡＮに対応する複数のルータまたはブリッジと、バックボーン網により構成され、各ＬＡＮは対応するルータまたはブリッジにより前記バックボーン網を介して互いに接続され、各ＬＡＮは基地局と１つ以上の無線端末を含む無線ネットワークにおける無線端末の認証方法であって、前記無線端末は、最初に通信を開始するにあたり、ＡＲＰのリクエ

ストまたはＤＨＣＰのリクエストを送信し、前記基地局は、そのリクエストを中継すると共に、送信元のＭＡＣアドレスを取り出して、認証サーバに対して端末の認証を行うためのパケットを送信し、前記認証サーバは、ＭＡＣアドレスを受信すると、あらかじめ配布しているシークレットキーで暗号化を行ったセッションキーを送信し、前記基地局は、セッションキーを保存すると共に、ＡＲＰのリプライまたはＤＨＣＰのレスポンスのパケットに、セッションキーをつけて送信し、前記無線端末は、受信したセッションキーを保存し、以降のパケット送信では、ＣＲＣ値の計算をＭＡＣのヘッダ、ペイロードにセッションキーを加えたハッシュ値を元に、計算してパケットを送信し、前記基地局は、パケット受信時に、保存しているセッションキーを使って、同様のＨＡＳＨ値を加えたＣＲＣ計算の値とパケットのＣＲＣの値を比較することで、パケット単位の認証を実現することを特徴とする。

【０００７】この発明によれば、ＩＰでの通信を開始するにあたり、無線端末が、ＡＲＰのリクエストまたはＤＨＣＰのリクエストを送信する。基地局（アクセスポイント）側では、このＡＲＰまたはＤＨＣＰパケットの送信元ＭＡＣアドレスを取り出して、認証サーバに対して端末の認証を依頼する。認証サーバは、ＭＡＣアドレスをチェックし、あらかじめ配布しているシークレットキーで暗号化したセッションキーを送信し、基地局は、セッションキーを保存すると共に、ＡＲＰのリプライまたはＤＨＣＰのレスポンスパケットにセッションキーをつけて送信する。無線端末は、受信したセッションキーを保存し、端末局はセッションキー入手以降、パケット送信時に、ＭＡＣフレームのＣＲＣの値を計算するにあたって、ＭＡＣヘッダ、ペイロードとセッションキーでＨＡＳＨ値を計算し、そのＨＡＳＨ値がペイロードの最後に付加されたパケットに対してＣＲＣを計算し、そのＣＲＣ値を通常のＭＡＣフレームのＣＲＣ値として送信を行う。基地局では、このパケットを受信した場合、受信したパケットのＭＡＣヘッダとペイロードとセッションキーから端末側の処理と同様にＨＡＳＨ値を計算し、それを加えてＣＲＣ値の計算を行い、受信したパケットのＣＲＣ値と比較を行って、パケット単位の認証を行う。したがって、パケット単位での認証が可能であり、事前に共有するセッションキーはパケットからは判別できないことから、無線ネットワーク上のパケットを盗み見て、なりすましによる不正アクセスを防止することが可能になる。また、パケットフォーマットに変更を行わないので、データリンクの最大転送可能データ長に影響を与えることはなく、利用者にはトランスペアレントである。

【０００８】また、請求項２に係る無線ネットワークにおける無線端末の認証システムは、複数のＬＡＮと、無線端末の認証を行う認証サーバと、バックボーン網とにより構成され、各ＬＡＮおよび認証サーバは対応するルータまたはブリッジにより前記バックボーン網を介して互いに接続され、各ＬＡＮは基地局と１つ以上の無線端末を含む無線ネットワークにおける無線端末の認証システムであって、前記無線端末は、最初に通信を開始する場合に、ＡＲＰのリクエストまたはＤＨＣＰのリクエストを送信する第１の送信手段と、前記基地局から受信したセッションキーを保存する第１の保存手段と、ＣＲＣ値の計算をＭＡＣのヘッダ、ペイロードにセッションキーを加えたハッシュ値を元に、計算してパケットを送信する第２の送信手段と、を備え、前記基地局は、前記無線端末からのリクエストを中継すると共に、送信元のＭＡＣアドレスを取り出して、前記認証サーバに対して端末の認証を行うためのパケットを送信する第３の送信手段と、前記認証サーバから受信したセッションキーを保存する第２の保存手段と、ＡＲＰのリプライまたはＤＨＣＰのレスポンスのパケットに、セッションキーをつけて送信する第４の送信手段と、パケット受信時に、前記第２の保存手段で保存しているセッションキーを使って、同様のＨＡＳＨ値を加えたＣＲＣ計算の値とパケットのＣＲＣの値を比較してパケット単位の認証を行う認証手段と、を備え、前記認証サーバは、ＭＡＣアドレスを受信すると、あらかじめ配布しているシークレットキーで暗号化を行ったセッションキーを送信する第５の送信手段を備えたことを特徴とする。

【０００９】

【発明の実施の形態】以下、本発明の無線ネットワークにおける無線端末の認証方法および無線端末の認証システムの一実施の形態について図面を参照して詳細に説明する。

【００１０】図１は、本発明の一実施の形態のネットワーク説明図である。本実施の形態のネットワークはＬＡＮ１１と無線ＬＡＮ１２とインターネット１３により構成され、ＬＡＮ１１と無線ＬＡＮ１２は、アクセスポイント１を介して互いに接続されている。なお、無線ＬＡＮ１２は、アクセスポイント１と無線端末２，３，４，５，６から構成される。ＬＡＮ１１はアクセスポイント１と認証サーバ７から構成される。

【００１１】図２は、図１のネットワークを構成する無線端末２～６の構成を示すブロック図である。無線端末２～６は、記憶装置２１とＣＲＣ計算部２２とパケット処理部２３と無線通信部２４とを備えている。記憶装置２１には、無線端末のＭＡＣアドレスと無線端末が通信する場合に利用するセッションキーを格納する。

【００１２】ＣＲＣ計算部２２は、パケット処理部がパケット送信において、パケットにつけるＣＲＣの計算を行う。ＣＲＣの計算は、図４に示すように、送信するパケットのＭＡＣヘッダとペイロードの部分とセッションキーの値を含めて、ＨＡＳＨ値の計算を行い、そのＨＡＳＨ値を送信パケットのＭＡＣヘッダとペイロード部分

の後に入れた形で、パケットのＣＲＣ値計算を行う。

【００１３】パケット処理部２３は、パケットの送受信を行うが、パケットの送信時に、前記のＣＲＣ計算部で計算したＣＲＣ値をパケットのＣＲＣの部分に添付して送信を行う。

【００１４】無線通信部２４は、パケット部から送信パケットを受け、無線ＬＡＮに対して送信処理を行い、また、無線ＬＡＮから受信するパケットをパケット処理部に通知する。

【００１５】図３は、図１のネットワークを構成するアクセスポイント１の構成を示すブロック図である。アクセスポイント１は、ＬＡＮ通信部３１とパケット処理部３２と無線通信部３４と記憶装置３４とＣＲＣ計算部３５とを備える。ＬＡＮ通信部３１は、アクセスポイント１が接続しているＬＡＮ１１へのパケットの送受信を制御する。パケット処理部３２は、ＬＡＮ１１から受信したパケットを、無線ＬＡＮ１２へ中継する処理を行う、また無線ＬＡＮ１２から受信したパケットをＬＡＮ１１に中継する。

【００１６】アクセスポイント１では、無線ＬＡＮ１２からパケットを受信した場合に、図４で無線端末が行う処理とは逆の処理を行う。受信において、ＭＡＣヘッダとペイロードの部分とセッションキーの値を含めてＨＡＳＨ値の計算を行い、そのＨＡＳＨ値を送信パケットのＭＡＣヘッダとペイロード部分の後に入れた形で、パケットのＣＲＣ計算を行って、受信パケットに含まれていたＣＲＣの値と一致するかどうかを確認する。一致する場合には、受信パケットをＬＡＮ１１に中継し、一致しない場合には、廃棄する。この動作により、セッションキーを持たない無線端末が無線ＬＡＮネットワークを利用して、インターネットへの接続を行うことを排除することが可能になる。

【００１７】前述したように本実施の形態によれば、パケット単位での認証が可能であり、かつ、事前に共有するセッションキーはパケットからは判別できないため、無線ネットワーク上のパケットを盗み見て、なりすましによる不正アクセスを防止することができる。また、パケットフォーマットに変更を行わないので、データリンクの最大転送可能データ長に影響を与えることはなく、利用者にはトランスペアレントであるという効果を奏する。

【００１８】さらに、セッションキーをＡＲＰやＤＨＣＰなどのリンク層以上のプロトコルのパケットに追加することによって、認証のためのトラヒックを増加を抑制することで、接続時間の短縮を行うことが可能となる。

【００１９】

【発明の効果】以上説明したように、本発明（請求項１および請求項２）によれば、ＩＰでの通信を開始するにあたり、無線端末が、ＡＲＰのリクエストまたはＤＨＣＰのリクエストを送信し、基地局（アクセスポイント側）では、このＡＲＰまたはＤＨＣＰパケットの送信元ＭＡＣアドレスを取り出して、認証サーバに対して端末の認証を依頼し、認証サーバが、ＭＡＣアドレスをチェックし、あらかじめ配布しているシークレットキーで暗号化したセッションキーを送信し、基地局では、セッションキーを保存すると共に、ＡＲＰのリプライまたはＤＨＣＰのレスポンスパケットにセッションキーをつけて送信し、無線端末が、受信したセッションキーを保存し、端末局はセッションキー入手以降、パケット送信時に、ＭＡＣフレームのＣＲＣの値を計算するにあたって、ＭＡＣヘッダ、ペイロードとセッションキーでＨＡＳＨ値を計算し、そのＨＡＳＨ値がペイロードの最後に付加されたパケットに対してＣＲＣを計算し、そのＣＲＣ値を通常のＭＡＣフレームのＣＲＣ値として送信を行い、基地局では、このパケットを受信した場合、受信したパケットのＭＡＣヘッダとペイロードとセッションキーから端末側の処理と同様にＨＡＳＨ値を計算し、それを加えてＣＲＣ値の計算を行い、受信したパケットのＣＲＣ値と比較を行って、パケット単位の認証を行うため、パケット単位での認証が可能であり、かつ、事前に共有するセッションキーはパケットからは判別できないことから、無線ネットワーク上のパケットを盗み見て、なりすましによる不正アクセスを防止することが可能になる。また、パケットフォーマットに変更を行わないので、データリンクの最大転送可能データ長に影響を与えることはなく、利用者にはトランスペアレントである。換言すれば、パケットフォーマットを変更することなく、不正なユーザによる不正アクセスを防止して、ネットワークリソースの不正利用を回避することができる。

【図面の簡単な説明】

【図１】本発明の一実施の形態のネットワーク説明図である。

【図２】図１のネットワークを構成する無線端末２～６の構成を示すブロック図である。

【図３】図１のネットワークを構成するアクセスポイント１の構成を示すブロック図である。

【図４】無線端末の送信時の処理であるＣＲＣの計算を示す説明図である。

【符号の説明】

１　アクセスポイント

２，３，４，５，６　無線端末

７　認証サーバ

１１　ＬＡＮ

１２　無線ＬＡＮ

１３　インターネット

２１　記憶装置

２２　ＣＲＣ計算部

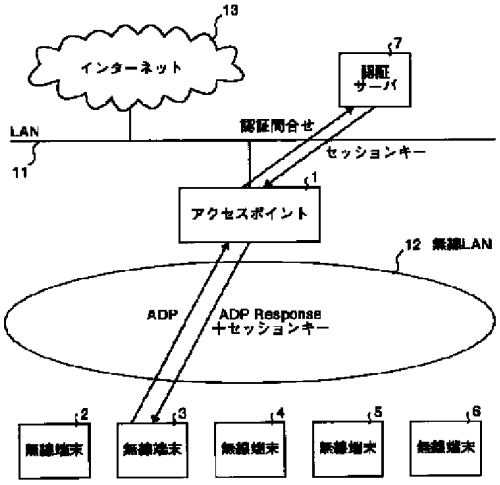
２３　パケット処理部

２４　無線通信部

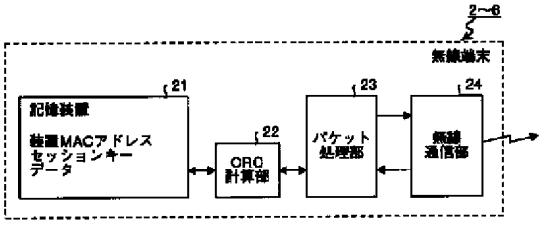
３１　ＬＡＮ通信部

３２　パケット処理部
３３　無線通信部
３４　記憶装置
３５　ＣＲＣ計算部

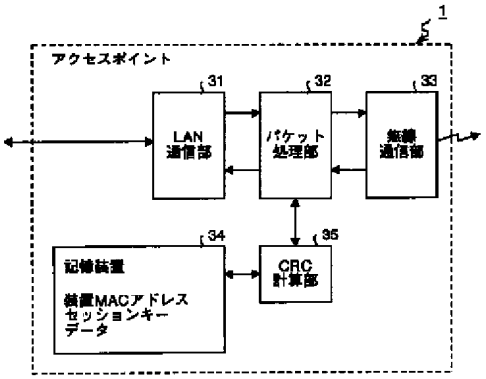
【図１】



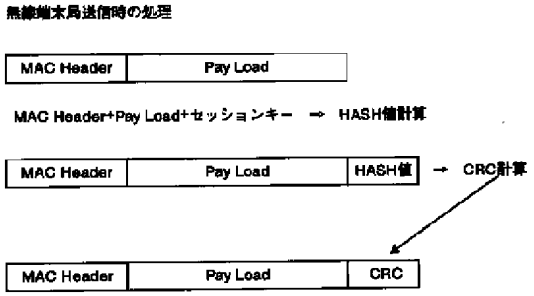
【図２】



【図３】



【図４】



フロントページの続き

(51)Int.Cl.7	識別記号	ＦＩ	テーマコード（参考）
		Ｈ０４Ｌ　11/20	１０２Ｚ

Fターム(参考)　5J104 AA07 AA16 EA04 EA18 EA22
KA02 KA06 MA01 NA03 NA12
PA01
5K030 GA15 HA08 HB12 HB28 HC14
HD03 HD07 JL01 LD19
5K033 AA08 CA08 DA05 DA17
5K067 AA30 BB21 CC08 DD13 DD17
DD51 EE02 EE10 HH23 HH26
HH36 KK15